UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/911,765	07/25/2001	Igor Muttik	01.042.01	5011

23117 7590 01/12/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
SANDOVAL, KRISTIN D	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/911,765	MUTTIK ET AL.	
	Examiner	Art Unit	
	Kristin D. Sandoval	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *48 and 49* is/are allowed.

6)☒ Claim(s) *1-47,50 and 51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/30/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-51 are pending.

Claim Rejections - 35 USC § 112

2. Amendments to the claims overcome the previous 112 rejections.

Response to Arguments

3. Applicant's arguments filed October 30, 2006 have been fully considered but they are not persuasive.

With regard to Applicant's arguments that Gryaznov fails to teach dividing an on-access malware scan into a plurality of tasks and a malware scanning task being one of a plurality of malware scanning tasks that are each part of an on-access malware scan, Examiner respectfully disagrees. Gryaznov discloses a virus scan that scans news messages for viruses. In order to complete the scan of the news messages, the virus scan is divided up into multiple tasks, these tasks consist of individual partitioned virus scans, where each virus scan is responsible for scanning a portion of the news messages where the scanning occurs in parallel (5:46-6:13).

With regard to Applicant's argument that Gryanzov fails to suggest issuing a plurality of tasks to be performed by a plurality of different computers, the Examiner respectfully disagrees. Gryaznov discloses the various tasks of virus scanning different partitions of the news messages occurring concurrently on a plurality of partition servers which constitute a plurality of different computers (6:1-13).

With regard to Applicant's argument that Gryaznov fails to disclose a plurality of malware scanning task results corresponding to a plurality of malware scanning tasks being collated to form a scan result corresponding to said on-access malware scan, Examiner respectfully disagrees. Gryaznov discloses each virus scanner, upon discovering any infected file, sending warning messages to a list of specified addressees, including the administrator for the virus scanners. Therefore, the results of each task, which consists of the partitioned virus scan, are collated at the administrator for all the virus scanners since the administrator receives all results in the form of warning messages (7:36-45).

With regard to Applicant's argument that Gartside fails to teach not further dividing an on-access malware scan if the malware scan is detected as having a complexity below a predetermined threshold level, Examiner respectfully disagrees. Gartside discloses a complexity level based on pre-compressed archive size, number of files within the archive and number of file types. If the levels of these factors are below a predetermined threshold then the overall complexity of the scan is below a certain threshold level and thus, the scan is not further divided beyond scanning for an excessive pre-compressed archive size, number of files with the archive and number of file types (6:25-64).

Allowable Subject Matter

4. Claims 48 and 49 allowed.

~~***Conclusion***~~

GR

scanners are identifying properties of a computer file since they are identifying viruses which are properties of the computer file that they are infecting).

As per claims 8, 23 and 38:

Gryaznov discloses a computer program product wherein the one or more tasks are further divided into sub-tasks (5:46-67, fig. 4a-4c, wherein the sequence of process steps are the tasks, which are the multiple virus scans into sub-tasks which are the processing steps that each virus scan is broken down into).

As per claims 12, 27, 42 and 50:

Gryaznov discloses a computer program product wherein the result collating logic terminates any outstanding tasks if a task result is received indicating detection of malware within said computer file (7:36-45).

As per claim 51:

Gryaznov discloses a computer program product wherein said plurality of tasks are distributed among said plurality of different computers via network (6:1-13).

Claim Rejections - 35 USC § 103

7. Claims 2-4, 9-11, 14, 17-19, 24-26, 29, 32-34, 39-41, 44 and 46-47 rejected under 35 U.S.C. 103(a) as being unpatentable over Gryaznov (U.S. 6,748,534) as applied to claims 1, 7, 13, 16, 22, 28, 31, 37 and 43 above, and further in view of Gartside, U.S. Patent No. 6,851,058.

As per claims 2-4, 14, 17-19, 29, 32-34 and 44:

Gryaznov fails to teach computer files being divided into component files that contain embedded computer files to also be component computer files wherein the computer file is one

of a given list of types. However, Gartside discloses a method wherein a computer file is an archive file and the archive file is broken down into its component files which are further broken down if embedded files exist in order to be scanned (3:36-50 wherein the files are extracted from the archive and are thus divided out from the file and if one of the files is thus embedded and is an archive, it is extracted for scan, therefore the computer file is divided into component computer files to be separately scanned, 4:39-48, 1:53-63).

As per claims 9-11, 24-26 and 39-41 and 46-47:

Gryaznov fails to teach where a task is selected to be issued to another computer in dependence upon one of a variety of reasons and the scan dividing logic does not divide the scan if the scan is detected as having a complexity below a predetermined threshold level and where the complexity is determined as a function of one or more of a list. However, Gartside discloses an archive file not being divided if it is below a certain complexity level (6:17-65) wherein the complexity level is determined as a function of the archive file (6:17-65), and a scan being selected to happen depends upon the storage space available (4:61-5:6).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the distributed scanning invention of Gryaznov with the archive scanning of Gartside because if the news database contained files with embedded files they could utilize a severe amount of processing power and memory space in order to scan through all of them (Gartside, 1:64-2:6). Therefore, the division of the embedded archive files would allow the news database to provide the processing and bandwidth throughput required by a growing dataset (Gryaznov, 2:33-40).

8. Claims 6, 21 and 36 rejected under 35 U.S.C. 103(a) as being unpatentable over Gryaznov as applied to claims 1 and 5 above, and further in view of Ranger et al. (Ranger), U.S. Patent No. 6,393,568.

As per claims 6, 21 and 36:

Gryaznov fails to teach the plurality of tasks seeking to identify different portion of one of a cryptographic analysis and an emulation analysis. However, Ranger discloses a method wherein a virus scans employs a cryptographic analysis in order to determine whether any unsolicited content is present within an encrypted file (2:25-46).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the invention of Ranger in combination with the invention of Gryaznov in order to detect viruses in encrypted news threads and thus increase the ability of the virus scanners to locate computer viruses in not only embedded computer files but also encrypted ones.

Allowable Subject Matter

9. Claims 48 and 49 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin D. Sandoval whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kristin D Sandoval
Examiner
Art Unit 2132

KDS

KDS

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100